

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
TAMPA DIVISION

UNITED STATES OF AMERICA

v.

Case No. 8:19-cr-33-T-36CPT

JACK R. DOVE, III

\_\_\_\_\_/

**REPORT AND RECOMMENDATION**

Before me on referral is *Defendant [Jack R. Dove, III's] Motion for a Hearing Pursuant to Franks v. Delaware*. (Doc. 83). For the reasons discussed below, I respectfully recommend that Dove's motion be denied.

I.

This action stems from an ongoing law enforcement investigation into a website predominantly used to host and distribute child pornography and child erotica (hereinafter, The Website).<sup>1</sup> (Doc. 83-2 at ¶¶ 18, 22-23). In connection with this investigation, the government sought and obtained a search warrant in November 2018 for Dove's residence in Lakeland, Florida (hereinafter, Subject Premises). (Doc. 83-1). The warrant authorized agents to search for evidence, contraband, and/or property relating to the distribution, receipt, and/or possession of child pornography, and was supported by the affidavit of United States

---

<sup>1</sup> The actual name of the Website is not specified herein because the government's investigation remains active. See (Doc. 83-2 at ¶ 18 n.5).

Department of Homeland Security Special Agent Tavey Garcia. *Id.*; (Doc. 83-2). Upon executing the warrant, the government seized a number of electronic and digital storage devices from the Subject Premises that contained child pornography. (Doc. 1 at ¶¶ 17-19; Doc. 93 at 7-8).

Dove was subsequently indicted on charges of receiving a visual depiction involving the use of a minor engaging in sexually explicit conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); and possessing and accessing a visual depiction involving the use of a prepubescent minor under the age of twelve engaging in sexually explicit conduct, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). (Doc. 17). Dove pleaded not guilty to these charges and was released on bond. (Docs. 11, 23).

Over the next roughly ten months, Dove requested and was granted multiple extensions of time to file pretrial motions. (Docs. 27-28, 33-34, 39-40, 50-51, 53-54, 73, 75, 80-81). Those extension requests were predicated, in substantial part, on Dove's need to obtain and review the government's voluminous discovery with his forensic computer expert. (Docs. 27, 33, 39, 50, 53, 73, 80). Of significance here, that discovery included a number of items referenced in Special Agent Garcia's affidavit, including The Website server itself, as well as an Excel spreadsheet of data extracted from The Website allegedly reflecting Dove's download of child pornography in August and September 2017. (Docs. 46 at 4-6, 53, 73, 80, 117-5).

By way of the instant motion, Dove now claims that he is entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) on the grounds that Special Agent Garcia’s affidavit omitted material facts and contained materially false statements made in reckless disregard for the truth. (Doc. 83). The government opposes Dove’s motion. (Doc. 93).

I held a series of initial hearings on Dove’s motion to address, in part, his request that the government disclose certain records he believed to be relevant to his motion. Following Dove’s receipt of those records, he sought and was granted leave to file a reply memorandum.<sup>2</sup> (Doc. 117). I subsequently conducted another hearing principally directed at the issues raised in Dove’s reply. The matter is now ripe for the Court’s consideration.

## II.

I begin with a summary of Special Agent Garcia’s affidavit, which states as follows. The Website is located on the darknet<sup>3</sup> and contains more than 125,000 unique videos for its users to download. (Doc. 83-2 at ¶¶ 18, 21). Although The Website “may” contain “some” adult pornography, law enforcement agents who have examined the site have found that the “overwhelming majority” of the images and videos on it appear to be child pornography or child erotica. *Id.* at ¶ 18. The

---

<sup>2</sup> The Court granted Dove leave to file two exhibits to his reply under seal. (Doc. 123). Those exhibits, F and G, consist of various bank records. (Doc. 124).

<sup>3</sup> A darknet is any online network that is accessible only through the use of specific software, configurations, or authorizations, and that is generally not accessible to users of the public, “open” internet. (Doc. 83-2 at ¶ 16). Darknet markets are typically commercial websites

Website's upload page instructs those who visit the site: "Do not upload adult porn."  
*Id.*

Not surprisingly given its content, The Website can only be accessed on the darknet via a computer network—known as "Tor"—that is specifically designed to facilitate anonymous communications over the internet.<sup>4</sup> *Id.* at ¶¶ 7, 16, 18. Tor accomplishes this by effectively "bouncing" a user's communications around a distributed network of relay computers all over the world. *Id.* at ¶ 7. The IP address of The Website, as well as those of The Website's users are hidden, such that there is no practical mechanism to trace a user's actual IP address. *Id.* at ¶ 7 & n.3.

Users may create a free account on The Website by providing a username and password. *Id.* at ¶ 19. To download videos from The Website, however, the user must expend "points," which can be acquired from The Website by, among other means, paying bitcoin (BTC).<sup>5</sup> *Id.*

BTC is a form of virtual currency and can be purchased from BTC virtual currency exchanges using conventional money. *Id.* at ¶¶ 8, 14. Virtual currency exchanges doing business in the United State are subject to the Bank Secrecy Act and must collect identifying information on their customers and verify their clients'

---

that primarily function as black markets, selling or brokering transactions involving illicit products, such as child pornography. *Id.* at ¶ 17.

<sup>4</sup> A user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle." *Id.* at ¶ 7.

<sup>5</sup> At the time of the affidavit, the cost of a "VIP" account on The Website (which entitled users to unlimited downloads for a period of six months) was .03 BTC (approximately \$125.58 as of September 2017), while incremental access could be purchased for lesser BTC amounts. *Id.* at ¶ 19.

identities. *Id.* at ¶ 14. Once acquired from a virtual currency exchange, however, BTC can be used in difficult-to-trace transactions as a payment method on the darknet, and is therefore one of the most common forms of payment within darknet markets. *Id.* at ¶¶ 9-14, 17.

BTC is sent to and received by BTC “addresses.” *Id.* at ¶ 9. A BTC address is somewhat analogous to a bank account number and is represented as a lengthy string of case-sensitive, alphanumeric characters. *Id.* Each BTC address is controlled with a unique “private key,” which is the cryptographic equivalent of a password or PIN needed to access the address, and only the holder of a BTC address’ private key can authorize a transfer of BTC from that address to another BTC address. *Id.*

To transfer BTC, the sender transmits a transaction announcement, cryptographically signed with the sender’s private key, across the peer-to-peer BTC network to another BTC address with its own private key. *Id.* at ¶ 10. The BTC address of the receiving party and a publicly identified key associated with the sender’s private key are the only pieces of information sent across the network to initiate and complete the transaction. *Id.* As a result, little to no personally identifiable data about the sender or recipient is revealed in a BTC transaction. *Id.* During its investigation, law enforcement found that The Website appeared to assign each user who accesses the site a unique BTC address to which the user could send funds (including BTC) to purchase account privileges. *Id.* at ¶ 20.

To locate and identify users of Tor-based websites like The Website, law enforcement relies on sophisticated commercial services offered by several different blockchain analysis companies. *Id.* at ¶¶ 11-15, 24. The blockchain is a decentralized public ledger, which logs every BTC address that has ever received BTC and maintains records of every transaction for each BTC address. *Id.* at ¶ 10.

Although the blockchain contains very little information about the BTC senders and recipients, blockchain analysis can be used to identify the individuals and entities involved in BTC transactions. *Id.* at ¶ 11. Blockchain analysis companies do this by creating large databases that group BTC transactions into “clusters” through the examination of the data underlying the BTC transactions. *Id.* at ¶ 12. As a result, law enforcement can utilize third-party blockchain analysis software to locate BTC addresses that transact at the same time (i.e., the blockchain logs transactions at the same time by two different BTC addresses) and then “cluster” these addresses together to represent the same owner. *Id.* at ¶¶ 13, 24. The third-party blockchain analysis software has supported many investigations and has been found to be reliable. *Id.* at ¶ 13.<sup>6</sup>

Because the blockchain serves as a searchable public ledger of every BTC transaction, law enforcement can trace these transactions to the BTC virtual currency exchanges, and then subpoena the exchange companies to obtain (at least in some

---

<sup>6</sup> For a general discussion of BTC and blockchain, see *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020) (holding that defendant lacked a privacy interest in his BTC transactions and affirming denial of motion to suppress).

instances) the true identity of the individuals responsible for the transactions. *Id.* at ¶ 15.

Using third-party blockchain analysis software, law enforcement agents identified nearly 3,000 unique BTC addresses clustered together (The Website cluster), which the software concluded to be associated with The Website. *Id.* at ¶ 24. Law enforcement agents corroborated this clustering analysis by following a controlled undercover payment of BTC from an agent's BTC wallet to a BTC address on The Website. *Id.* The third-party blockchain analysis software added this undercover transaction to The Website cluster. *Id.*

The third-party blockchain software showed that, between approximately October 2015 and February 2018, The Website cluster received approximately 411 BTC through 7,786 transactions from 4,255 different BTC addresses worth approximately \$324,961. *Id.* at ¶ 25. These payments included BTC sent to BTC addresses within The Website cluster directly from BTC addresses created through virtual currency exchanges. *Id.*

As part of its investigation of The Website, law enforcement subpoenaed business records from a United States-based BTC virtual currency exchange. *Id.* at ¶ 27.<sup>7</sup> Those records evidenced that a BTC exchange account, created on or about November 16, 2016, and linked to eight different BTC addresses as well as multiple IP addresses, was registered to "Jack Dove" at the Subject Premises. *Id.* The

---

<sup>7</sup> Although not specified in the Affidavit, the name of this BTC virtual currency exchange is Coinbase (Doc. 93-2), and it is sometimes referred to by the parties in their submissions as such, *see, e.g.*, (Doc. 93 at 4-5; Doc. 117 at 2).

records also included a telephone number associated with Dove, as well as an email address (jdove@totalonguardprotection.com) affiliated with a Dove-owned business (Total OnGuard Protection, LLC), which listed the Subject Premises as its registered address. *Id.* at ¶¶ 27, 34 n.10.<sup>8</sup> In addition, the payment details for the account identified three Master Card debit/credit cards, two of which had a billing address of the Subject Premises. *Id.* at ¶ 28.

The blockchain analysis software determined that this BTC account registered to Dove (hereinafter, Dove's BTC account) engaged in multiple transactions with a BTC address within The Website cluster between on or about November 16, 2016, and on or about August 23, 2017. *Id.* at ¶ 29. Additional data extracted from The Website, which was provided to Special Agent Garcia in October 2018, revealed Dove had downloaded approximately twenty child-pornographic videos on or about August 10, 2017, and approximately eighteen child-pornographic videos on or about September 3, 2017. *Id.* at ¶ 30.

In advance of seeking a search warrant for the Subject Premises, law enforcement agents determined that Dove purchased the Subject Premises in 2011; that Dove and another adult with Dove's last name listed the Subject Premises on their driver's licenses; and that one of the IP addresses identified in Dove's BTC account was associated with "Jack Dove" at the Subject Premises between June 6

---

<sup>8</sup> Dove voluntarily dissolved Total OnGuard Protection in June 2017 and created a fictitious business name, Our Secret Toys, which also listed the Subject Premises as its registered address. *Id.* at ¶ 34 n.10. That business name was active at the time of the search warrant's submission. *Id.*



and August 18, 2017. *Id.* at ¶¶ 31-33. In addition, agents conducting surveillance of the Subject Premises during the three weeks leading up to the submission of the search warrant observed, among other things, two vehicles known to be affiliated with Dove and his business, including one for which Dove was the primary driver. *Id.* at ¶¶ 34-37.

At the time she submitted the warrant to the issuing magistrate judge, Special Agent Garcia also knew from her training, experience, and information supplied by other knowledgeable law enforcement agents that individuals who have a sexual interest in children or images of children and who utilize the web to access with the intent to view, possess, receive, or distribute images of child pornography, almost always possess and maintain their child pornographic materials “for many years” in the privacy and security of their homes or some other secure locations. *Id.* at ¶¶ 36, 41(c), (d).<sup>9</sup> She was also aware that evidence of such an individual’s downloading, viewing, and even deletion of child pornography can often be located on the individual’s computers and digital devices for extended periods of time through the use of forensic tools. *Id.* at ¶¶ 36, 41(e).

### III.

The Fourth Amendment to the United States Constitution provides that “no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be

---

<sup>9</sup> Paragraphs 36 through 39 on pages 23 to 31 of the affidavit are misnumbered and repeat the preceding paragraph numbers.

seized.” U.S. Const. amend. IV. Probable cause exists where the totality of the circumstances would justify a prudent person in believing that there is a “fair probability” that contraband or evidence of a crime will be found in the place to be searched. *Florida v. Harris*, 568 U.S. 237, 243-44 (2013); *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

In assessing whether probable cause exists, “as the very name implies, [judges] deal with probabilities.” *Brinegar v. United States*, 338 U.S. 160, 175 (1940). Such probabilities “are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent [people], not legal technicians, act.” *Id.* Probable cause is therefore viewed as “a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *Gates*, 462 U.S. at 232.

As a result, the task of a magistrate in evaluating a search warrant “is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the ‘veracity’ and ‘basis of knowledge’ of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238-39 (citing and quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). In conducting this analysis, the magistrate should look at the “affidavit as a whole” and “in a realistic and non-technical manner,” and should “not read[ ] words and phrases . . . out of the context in which they were written.” *United States v. Joyce*, 2012 WL

7148366, at \*2 (S.D. Fla. Dec. 12, 2012) (citations omitted), *report and recommendation adopted*, 2013 WL 560817 (S.D. Fla. Feb. 13, 2013).

Once issued, search warrants are presumed to be valid. *Franks*, 438 U.S. at 171. “And the duty of a reviewing court is simply to ensure that the magistrate had a ‘substantial basis for . . . conclud[ing]’ that probable cause existed.” *Gates*, 462 U.S. at 238-39 (quoting *Jones*, 362 U.S. at 271); *see also Massachusetts v. Upton*, 466 U.S. 727, 732-33 (1984) (per curiam) (noting that, in determining whether probable cause existed to justify a warrant, a reviewing court should not review the magistrate’s determination de novo but should assess “whether the evidence viewed as a whole provided a ‘substantial basis’ for the [m]agistrate’s finding of probable cause”). As the Supreme Court explained in *Gates*:

[A]fter-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review. A magistrate’s determination of probable cause should be paid great deference by reviewing courts. . . . [and] courts should not invalidate . . . warrant[s] by interpreting affidavit[s] in a hypertechnical, rather than a commonsense, manner.

462 U.S. at 236 (internal quotation marks and citations omitted).

Consistent with this admonition, a reviewing court should not insist that a search warrant adhere to an unrealistic level of precision or exactitude. As one court aptly noted:

Affidavits and warrants, which are frequently drafted under time pressure, often by police or persons without legal training, and which must frequently express complex thoughts, cannot properly be subjected to the same standards of dissection as might befit a criminal statute, an indictment, or a trust indenture.

*Nat'l City Trading Corp. v. United States*, 487 F. Supp. 1332, 1336 (S.D.N.Y. 1980), *aff'd*, 635 F.2d 1020 (2d Cir. 1980); *see also United States v. Carmel*, 548 F.3d 571, 575 (7th Cir. 2008) (“[P]erfection is not required for a[ search warrant] affidavit to pass constitutional muster. Rather, the affidavit only must be sufficient to allow a reasonably prudent person to believe that evidence of a crime will be found.”) (citation omitted).

One of the ways a defendant may challenge the validity of a search warrant is through the procedure first enunciated by the Supreme Court in *Franks*. In that case, the Court established:

[W]here the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

438 U.S. at 155-56.

The requirement of the hearing referenced in *Franks* also extends to situations where facts are intentionally or recklessly omitted from a warrant if the “inclusion of the omitted facts would have prevented a finding of probable cause.” *United States v. Lebowitz*, 676 F.3d 1000, 1010 (11th Cir. 2012) (per curiam) (quoting *United States v. Kapordelis*, 569 F.3d 1291, 1309 (11th Cir. 2009)). Insignificant, immaterial, or even negligent misrepresentations or omissions, on the other hand, do not trigger the need for a further *Franks* inquiry. *United States v. Williams*, 146 F. App'x 425, 430

(11th Cir. 2005)<sup>10</sup> (per curiam) (citing *United States v. Reid*, 69 F.3d 1109, 1114 (11th Cir. 1995)); *United States v. Sims*, 845 F.2d 1564, 1571 (11th Cir. 1988) (citation omitted).

Thus, to be entitled to a *Franks* hearing, a defendant must make a “‘substantial preliminary showing’ that (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the challenged statement or omission was essential to the finding of probable cause.” *United States v. Arbolaez*, 450 F.3d 1283, 1293 (11th Cir. 2006) (per curiam) (citing *Franks*, 438 U.S. at 155-56). A defendant must satisfy both of these prongs to be entitled to an evidentiary hearing. *Id.*

The substantial preliminary showing required by *Franks* “is not lightly met.” *Id.* at 1294. As the Eleventh Circuit has made clear:

To mandate an evidentiary hearing, the challenger’s attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.

*Id.* (quoting *Williams v. Brown*, 609 F.2d 216, 219 (5th Cir. 1979)).

---

<sup>10</sup> Unpublished opinions are not considered binding precedent but may be cited as persuasive authority. 11th Cir. R. 36-2.

If such a showing is made, “the trial court is to disregard those portions of the affidavit which the defendant has shown are arguably false or misleading.” *Kapordelis*, 569 F.3d at 1309 (citing *Franks*, 438 U.S. at 171-72). “Looking only at the remaining portions of the affidavit, the court will then determine whether including the omitted facts would have prevented a finding of probable cause.” *Id.* (citation omitted). If probable cause still exists once the misrepresentations are removed from the warrant and the omissions are inserted, there is no *Franks* violation and no need for a hearing. *United States v. Capers*, 708 F.3d 1286, 1296 (11th Cir. 2013) (citation omitted); *Lebowitz*, 676 F.3d at 1010-11.

A court’s denial of a *Franks* hearing is reviewed on appeal for an abuse of discretion. *United States v. Barsoum*, 763 F.3d 1321, 1328 (11th Cir. 2014), *cert. denied*, 575 U.S. 978 (2015).

#### IV.

In support of his request for a *Franks* hearing, Dove posits the following arguments: (a) Special Agent Garcia recklessly misrepresented and/or omitted pertinent information regarding the Master Card debit/credit card numbers associated with Dove’s BTC account; (b) Special Agent Garcia recklessly failed to disclose that one of the IP addresses tied to Dove’s BTC account was not affiliated with the Subject Premises at certain relevant periods, and that the Internet Service Provider (ISP) records upon which the agent based her representations were unreliable; (c) Special Agent Garcia’s description of the details regarding Dove’s BTC account did not accurately reflect the account information in existence at the

time of the alleged conduct involving The Website; and (d) Special Agent Garcia recklessly misrepresented that Dove downloaded approximately twenty child-pornographic videos on or about August 10, 2017, and approximately eighteen child-pornographic videos on or about September 3, 2017. (Doc. 83 at 5-7, 12; Doc. 117 at 6-11, 16-17). Each of these arguments is addressed in turn below.

A.

Dove claims that the Master Card debit/credit card information in Special Agent Garcia's affidavit is false or incomplete in three respects: (a) the last four digits of the account numbers are wrong; (b) the affidavit did not reveal that other individuals were associated with those debit/credit card accounts; and (c) at least one of the debit/credit cards was associated with another address in addition to the Subject Premises. (Doc. 83 at 2, 7-8, 12; Doc. 117 at 2, 5-6, 11-12, 16-17).

The pertinent allegations relating to these Master Card debit/credit cards are found in paragraphs 27 and 28 of the affidavit. These paragraphs state:

27. Business records returned after a subpoena was served on a United States based BTC exchange revealed that a BTC User with ID number 582c6601c8aldb3f8e0147ld, created on or about November 16, 2016, was registered to "Jack Dove" ("DOVE") at the SUBJECT PREMISES. The registration information for the BTC exchange account also included the email address "jdove@totalonguardprotection.com," a telephone number associated with DOVE, and internet protocol (IP) addresses including, but not limited to: 70.127.40.255 . . .

\* \* \*

28. The above-mentioned [BTC] account also contained the following payment card details:

- a. Master card debit card, ending in 2019, issued by Bank of America with the billing address: SUBJECT PREMISES.
- b. Master card, ending in 2020, issued by Citibank with the billing address: SUBJECT PREMISES.
- c. Master card debit card, ending in 2021, issued by Bank of America.

(Doc. 83-2 at ¶¶ 27-28).

As the government concedes, the listed card numbers in paragraph 28 are not correct, insofar as they represent the cards' years of expiration, not the last four digits of the cards' account numbers. (Doc. 93 at 13). The fact that these card numbers are wrong, however, does not end the inquiry. Dove must make a substantial preliminary showing that Special Agent Garcia provided this inaccurate information intentionally or in reckless disregard of the truth, and that excluding this information would preclude a finding of probable cause. Dove shows neither. The misstated card numbers appear to represent nothing more than a scrivener's error and are hardly relevant, much less vital, to the magistrate judge's probable cause determination. *Williams*, 146 F. App'x at 430 (noting that insignificant, immaterial, or even negligent misrepresentations or omissions do not provide cause for a *Franks* hearing).

Dove's claim that other individuals were associated with these debit/credit cards likewise does not amount to a *Franks* violation. According to Dove's submissions, records subpoenaed from Bank of America—which issued two of the three cards—reveal there were four accounts at that financial institution linked to



Dove. (Doc. 124). Three of these accounts were in Dove's and his mother's name, while the fourth was in his name, his mother's name, and the name of his wife, Melissa Dove.<sup>11</sup> (Docs. 124, 117 at 12). Dove argues that, although Special Agent Garcia was aware of this information, she failed to disclose to the issuing magistrate judge that "up to three persons potentially had access to cards used to fund the BTC transactions" (Doc. 117 at 12) and that these cards "may have been used for the purchase of child pornography" (Doc. 83 at 2).

There a number of problems with this argument. As an initial matter, by Dove's own records, the only two individuals besides him associated with the Bank of America cards are his mother and his wife, and there is no evidence before the Court (either in Dove's submissions or in Special Agent Garcia's affidavit) to suggest that either of these two women were aware of Dove's BTC account, much less "funded" BTC transactions for the purpose of viewing or downloading child pornography.<sup>12</sup>

Even were that not the case, the fact that two of Dove's family members are linked to the Bank of America debit cards is hardly fatal to the probable cause analysis. To begin, Dove's offer of proof pertains solely to the Bank of America

---

<sup>11</sup> Dove's wife is identified in the complaint and in Exhibit C to Dove's motion as "MD." (Doc. 1 at 10; Doc. 83-3).

<sup>12</sup> It bears emphasizing in this regard that, as noted above, BTC addresses (like those associated with Dove's BTC account) are controlled with a unique private key, and only the holder of a BTC address' private key can authorize a transfer of BTC from that address to another BTC address. (Doc. 83-2 at ¶ 9). Dove does not offer any proof that either his wife or his mother had access to the private key for his BTC addresses.

debit cards. He makes no allegation or showing that there were any other individuals connected to the third card identified in Dove's BTC account records issued by Citibank. And, as noted above, that card—like one of the two Bank of America cards—also listed the Subject Premises as its billing address.

Furthermore, the information in the Bank of America records upon which Dove relies (Doc. 124) does not undermine Special Agent Garcia's statement that both of the cards from that institution were linked to Dove's BTC account and, in the case of one of them, the Subject Premises as well. Notably, Dove does not contest that he is an authorized user of the Bank of America cards, or that he is the sole registrant for his BTC account.

More broadly, the search warrant in this case was for the Subject Premises, not for Dove's person. As a result, the fact that the Bank of America cards are listed to Dove and two of his loved ones is of comparatively little significance given that the primary import of the debit/credit card information is that it links the Subject Premises to Dove's BTC account, which in turn is tied to The Website.

Dove's contention that he is entitled to a *Franks* hearing because at least one of the Bank of America cards was associated with another address in addition to the Subject Premises is also unavailing. Notably, the Bank of America records upon which Dove predicates this assertion do not extend past April 2018, which is roughly seven months prior to the submission and execution of the search warrant. Dove makes no offer of proof that he resided at the second address at any point in time, much less in the months leading up to the signing of the warrant.

Putting aside this deficiency, the fact that there are Bank of America records linking Dove to a second physical address does not materially detract from all the other information in the affidavit tying him to the Subject Premises. This information includes that Dove purchased the Subject Premises in 2011; that he listed the Subject Premises on his driver's license; that two of three debit/credit cards associated with his BTC account identify the Subject Premises as the billing address; that the Subject Premises is the registered address for both his former and current businesses; and that vehicles associated with him (including one for which he was the primary driver) were observed at the Subject Premises during the weeks immediately prior to the submission and execution of the search warrant. (Doc. 83-2 at ¶¶ 31-39).

B.

Dove next claims Special Agent Garcia failed to disclose that, according to the records supplied by ISP Charter Communications (Charter), the IP address she cited in her affidavit (i.e., 70.127.40.225) was not associated with the Subject Premises until six months after the creation of Dove's BTC account and was terminated two weeks before at least one of the alleged child pornographic downloads. (Doc. 83 at 8-10; Doc. 117 at 12-16). Dove further maintains that Charter's records are unreliable in any event based on a disclaimer the ISP included with the records. That disclaimer stated:

Charter's billing and customer records from which the above information is obtained are subject to human error and Charter cannot always guarantee the accuracy of such records. You should not rely

solely on this information and should always independently corroborate the information Charter provides with other information you have concerning the identity of the individual.

(Doc. 83-5).

Dove's argument misapprehends both the nature of Special Agent Garcia's IP-related averments as well as the pertinence of the cited IP address itself. Special Agent Garcia first references the 70.127.40.225 IP address in paragraph 27 of her affidavit as one of a number of IP addresses linked to Dove's BTC account (Doc. 83-2 at ¶ 27),<sup>13</sup> and later states that, according to Charter's records, this particular IP address was associated with Dove and the Subject Premises between on or about June 6, 2017, and August 18, 2017, *id.* at ¶ 33. Contrary to Dove's suggestion, Special Agent Garcia does not state that this IP address was affiliated with Dove and the Subject Premises beyond this date range. As such, Special Agent Garcia's representations would not have misled the issuing magistrate judge as to the limited duration in which the 70.127.40.225 IP address was associated with Dove and the Subject Premises.

Dove also does not establish, as required under *Franks*, that the time frame during which the 70.127.40.225 IP address was linked to the Subject Premises was necessary to the magistrate judge's probable cause finding. By my reading of the affidavit, the IP address information simply provides additional evidence of the

---

<sup>13</sup> More particularly, Special Agent Garcia avers in paragraph 27, in pertinent part, that the registration information for Dove's BTC account listed IP "addresses, including, *but not limited to*: 70.127.40.225." (Doc. 83-2 at ¶ 27) (emphasis added).

connection between Dove, his BTC account, and the Subject Premises, including during the period in which Dove's BTC account engaged in BTC transactions with a BTC address within The Website cluster. (Doc. 83-2 at ¶¶ 29, 33). Even were the Court to excise from the affidavit the temporal limitation related to the IP address, it would not vitiate the magistrate judge's probable cause finding.

I reach the same conclusion with respect to the alleged unreliability of the Charter records. By my consideration, the inclusion of the disclaimer upon which Dove relies does not undermine the probable cause supporting the warrant. Consistent with that disclaimer, Special Agent Garcia did not rely solely on the Charter information to link Dove to the Subject Premises but instead independently corroborated that connection through multiple other means, including—as noted above—Dove's driver's license, his BTC account records, the property records for the Subject Premises, and surveillance of the Subject Premises. *See, e.g., id.* at ¶¶ 27-28, 31-39.

### C.

At the most recent hearing, Dove's counsel offered a different falsity argument with respect to the BTC account information contained in paragraph 27 of Special Agent Garcia's affidavit. While acknowledging Special Agent Garcia accurately described in that paragraph the information contained in the subpoenaed records for Dove's BTC account, Dove contends this does not mean that her representations correctly reflected the account information in existence at the time of the alleged child pornographic downloads. In support of this contention, Dove

asserts, *inter alia*, that the Subject Premises information identified in paragraph 27 was not added to Dove's BTC account until August 6, 2017.<sup>14</sup> This argument is also without merit.

As noted, to satisfy *Franks'* first prong, a defendant must make a substantial preliminary showing that the affiant deliberately or recklessly made a false allegation. Here, Dove fails to demonstrate that he was not living at the Subject Premises at the time he established his BTC account.

Even were that not the case, applying *Franks'* second prong, the mere fact that the Subject Premises information was added to Dove's BTC account on August 6, 2017, is not essential to the probable cause finding. As noted above, there is an abundance of evidence contained in the affidavit tying Dove to the Subject Premises. In addition, Special Agent Garcia's affidavit establishes probable cause to believe that Dove's BTC account was linked to The Website and to child-pornographic downloads from that site *after* August 6, 2017. *See* (Doc. 83-2 at ¶¶ 29-30 (referencing BTC transactions between Dove's BTC account and a BTC address within The Website cluster, as well as Dove's downloading of numerous child pornographic videos from The Website after August 6, 2017)).

D.

Dove's final *Franks* challenge focuses on paragraph 30 in the affidavit. (Doc. 83 at 5-7; Doc. 117 at 6). In that paragraph, Special Agent Garcia alleges:

---

<sup>14</sup> The government did not contest this factual assertion at oral argument.

On or about October 9, 2018, I received additional data that had been extracted from The Website, which revealed that DOVE had downloaded approximately 20 child-pornographic videos on or about August 10, 2017 and approximately 18 child-pornographic videos on or about September 3, 2017. . . .

(Doc. 83-2 at ¶ 30). Special Agent Garcia goes on to describe in the remainder of the paragraph three examples of the child pornographic videos “Dove” allegedly downloaded on August 10 and September 3, 2017. *Id.*

Dove argues he is entitled to a *Franks* hearing with respect to these averments because, at the time the affidavit was executed, Special Agent Garcia purportedly did not have any information to support her statement that Dove was the individual who actually downloaded the child pornographic content referenced in the paragraph. (Doc. 83 at 5-7). In support of this assertion, Dove states that the “additional data” to which Special Agent Garcia refers in the paragraph and which Dove has since obtained from the government only identifies the alleged downloader by the username “notus.” (Doc. 117 at 6-11, 14, 16, 18-19); (Doc. 117-5). And, Dove maintains, nothing in the government’s discovery shows that law enforcement had linked him to that username prior to the search warrant’s submission to the issuing magistrate judge. *Id.*; *see also* (Doc. 83 at 6).

The government countered at the most recent hearing that all of the information contained in paragraph 30 is true. It also represented that the “additional data” extracted from The Website, which was provided to Special Agent Garcia in October 2018, was forensically linked to Dove at the time.

While it is rather surprising that the government apparently does not have any discovery (such as a law enforcement report) related to the circumstances surrounding Special Agent Garcia's receipt of the "additional data," there are a number of aspects of Dove's falsity argument that give me pause. To begin, it is not entirely clear what, if any, any information in paragraph 30 is actually false. *United States v. Owden*, 345 F. App'x 448, 454 (11th Cir. 2009) (per curiam) (noting that "[t]he Fourth Amendment is violated if a warrant is obtained by using a *false* statement that was made intentionally or recklessly," and rejecting defendant's *Franks* challenge because the affiant's statements "were an accurate representation" of the evidence in question) (emphasis added) (citing *Franks*, 438 U.S. at 155-56), *cert. denied*, 559 U.S. 1084 (2010); *United States v. Nejad*, 436 F. Supp. 3d 707, 722 (S.D.N.Y. 2020) (finding defendant's *Franks* argument "meritless because it fail[ed] to even identify any false statements or omitted truths, prerequisites to the application of the *Franks* doctrine") (citation omitted); *United States v. Saunders*, 2019 WL 4040623, at \*2 (E.D. Va. Aug. 27, 2019) (explaining that "[a] critical prerequisite to [the] entitlement to a *Franks* hearing is a demonstration by a defendant . . . 'that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit'" (quoting *Franks*, 438 U.S. at 155-56), *appeal docketed*, No. 19-4882 (4th Cir. Dec. 4, 2019). Dove does not dispute, for example, that the "additional data" Special Agent Garcia received was extracted from The Website and evidences that approximately twenty child-pornographic videos were downloaded on or about August 10, 2017, and



approximately eighteen child-pornographic videos were downloaded on or about September 3, 2017. Nor does Dove contest that an individual employing the username “notus” was the one who downloaded these videos. And, as was apparent at the most recent hearing, he does not even dispute that he is “notus.”

Dove’s argument also gives me pause to the extent it improperly seeks to shift the burden to the government to prove the veracity of Special Agent Garcia’s averments, whether through its discovery disclosures or otherwise. *Franks* makes clear that it is the defendant’s obligation to make a substantial preliminary showing of falsity in order to satisfy *Franks*’ first prong, not the government’s burden of making a substantial preliminary showing of truthfulness to defeat that prong. *Franks*, 438 U.S. at 155-56; *United States v. Green*, 2020 WL 1983720, at \*8 (M.D. Fla. Apr. 27, 2020) (“A defendant who fails to make th[e requisite] ‘substantial preliminary showing’ is not entitled to a *Franks* hearing.”) (citing *Barsoum*, *supra*).

Moreover, the operative inquiry is not, as Dove seems to suggest, whether Special Agent Garcia correctly identified Dove as the downloader of the child pornography referenced in paragraph 30, but whether the agent “believed or appropriately accepted [the information set forth in that paragraph] as true.” *Franks*, 438 U.S. at 165 (citations omitted); *see also United States v. Flowers*, 531 F. App’x 975, 981 (11th Cir. 2013) (per curiam) (“*Franks* requires the defendant to offer proof that the affiant had the requisite intent.”) (citing *Franks*, 438 U.S. at 171). The *Franks* court adopted this standard recognizing that “probable cause may be founded upon hearsay and upon information received from” third parties. 438 U.S. at 165.

Here, while Special Agent Garcia could have made it clearer, a commonsense reading of paragraph 30 based on the affidavit taken as a whole (and the reasonable inferences to be drawn therefrom) is that Special Agent Garcia was provided this additional data after it had been forensically extracted by others from The Website, and that she believed the data at the time to pertain to Dove. For example, in the paragraphs leading up to and including paragraph 30, Special Agent Garcia indicates that she simply “received” this data; that she understood that Dove’s BTC account had already been linked by that point to eight different BTC addresses and at least eight BTC transactions; and that she further understood the third party “blockchain analysis software” had also determined by that juncture “that [Dove’s BTC account had] engaged in transactions with a BTC address within The Website cluster” between November 2016 and August 2017. (Doc. 83-2 at ¶¶ 27-30).

It is likewise noteworthy that, despite having his own computer forensic expert, Dove has not tendered any affidavits or other reliable witness statements supporting his *Franks* challenge to the veracity of the information contained in paragraph 30. Nor has Dove provided a satisfactory explanation as to why he has not included such affidavits and statements with his submissions. *Franks*, 438 U.S. at 171 (noting that “[a]ffidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained” by a defendant seeking a *Franks* hearing); *see also Arbolaez*, 450 F.3d at 1294 (“There is no affidavit or otherwise sworn statement alleging that [the affiant] knowingly or recklessly included false statements in the search warrant affidavit. Accordingly, we find that

[the defendant] has failed to make the necessary ‘substantial preliminary showing’ and that there is no error.”).

I am similarly unpersuaded by Dove’s falsity argument that takes issue with Special Agent Garcia’s use of the shorthand “Dove” in paragraph 30. Claiming that this designation misrepresents the evidence Special Agent Garcia had before her at the time she wrote the affidavit, Dove cites one of the earlier paragraphs in the affidavit where Special Agent Garcia averred that, “[b]ased on the instant investigation[,] there [wa]s probable cause that *an internet user associated with the SUBJECT PREMISES* has engaged in BTC transactions with BTC addresses within The Website cluster. . . .” (Doc. 83 at 6) (citing Doc. 83-2 at ¶ 26<sup>15</sup>).

Contrary to Dove’s contention, however, it is reasonable and logical to conclude, especially under the probable cause standard, that “an internet user” engaging in BTC transactions using a BTC account registered only in Dove’s name (as alleged in the affidavit) was Dove himself, particularly given that this account also listed Dove’s business email address, his telephone number, and two debit/credit cards billed to the Subject Premises where Dove resided. That virtual currency exchanges doing business in the United States—like the one used by Dove to create his BTC account—are legally required to “verify their clients’ identities” further buttresses this conclusion. (Doc. 83-2 at ¶¶ 14, 27). Under such circumstances, to employ the name Dove as a shorthand in paragraph 30 is not materially false when the affidavit is read as a whole and in context. *Joyce*, 2012

---

<sup>15</sup> This is the second of two paragraphs numbered 26 in the affidavit.

WL 7148366, at \*2 (noting that a magistrate judge should “utilize common sense to construe a search warrant affidavit in a realistic and non-technical manner,” and should look at the “affidavit as a whole,” and “not read[ ] words and phrases . . . out of the context in which they were written”) (citations omitted).

Nor would the issuing magistrate judge have mistakenly inferred from Special Agent Garcia’s shorthand reference to Dove in paragraph 30 that law enforcement had definitively identified Dove as the downloader of the child pornography at issue. This is especially true since, as Dove himself points out, Special Agent Garcia made clear in an earlier paragraph that the investigation had only developed probable cause to believe “an internet user associated with the Subject Premises” had engaged in the referenced BTC transactions with The Website Cluster (Doc. 83-2 at ¶ 26).

In any event, as discussed above, the search warrant in this case was for the Subject Premises, not for Dove’s person. As such, Special Agent Garcia’s assertion in paragraph 30 that “Dove,” as opposed to “an internet user associated with the Subject Premises,” downloaded the child pornography would not have changed the probable cause analysis.

In light of the above, it is not clear that Dove’s challenge to the averments in paragraph 30 satisfies *Franks*’ first prong. The Court need not resolve this issue, however, because it is evident that Dove’s challenge does not meet *Franks*’ second prong. Even without paragraph 30, the remaining information set forth in the affidavit is sufficient to establish probable cause for the requested search warrant.

That remaining information, and the reasonable inferences to be drawn therefrom, establish the following:

- The darknet is an online network that is accessible only through the use of specific software or network configurations, and that is generally not accessible to users of the public, “open” internet. (Doc. 83-2 at ¶ 16). Tor is an example of such specific software or network configurations, and is designed specifically to facilitate anonymous communications over the internet. *Id.* at ¶¶ 7, 16. A user must install Tor software either by downloading an add-on to the user’s web browser or by downloading the free “Tor browser bundle.” *Id.* at ¶ 7.

- Darknet markets are typically commercial websites operating as Tor hidden services that primarily function as black markets, selling or brokering transactions involving illicit products such as child pornography. *Id.* at ¶ 17. BTC is one of the most common methods of payment for products or services within darknet markets. *Id.*

- The Website is located on the darknet with a Tor-based website address and is predominantly—if not “overwhelmingly”—used to host and distribute video files depicting child pornography. *Id.* at ¶ 18.

- The Website is not accessible through standard search protocols. Instead, for a user to access The Website, they must know the specific web address of The Website, download Tor software, access the dark web, and affirmatively locate The Website’s web address. *Id.* at ¶ 18 n.6.

- Users may create a free account on The Website by providing a username and password. *Id.* at ¶ 19. The Website assigns each user who accesses the site a unique BTC address to which the user can send BTC to purchase account privileges. *Id.* at ¶ 20.

- While users may create a free account on the Website, only users who have acquired account privileges on The Website can download child pornographic videos from the site. *Id.* at ¶ 19.

- BTC addresses are controlled with a unique private key and only the holder of a BTC address' private key can authorize the transfer of BTC from that address to another BTC address. *Id.* at ¶ 9.

- Using reliable third-party blockchain analysis software, law enforcement identified nearly 3,000 unique BTC addresses clustered together (The Website cluster), which the software found to be associated with The Website. *Id.* at ¶ 24.

- The BTC payments received by The Website cluster during the period between in or around October 2015 and in or around February 2018 included payments sent to BTC addresses within The Website cluster directly from addresses created through virtual BTC currency exchanges. *Id.* at ¶ 25.

- Records subpoenaed from a United States-based BTC virtual currency exchange revealed that a BTC account registered to "Jack Dove" was created on or about November 16, 2016, with an email address and telephone number associated with Dove, and with debit/credits card associated with the Subject Premises. *Id.* at

¶ 27. As required by law, the United States-based BTC exchange verified Dove's identity. *Id.* at ¶ 14.

- The blockchain analysis software determined that BTC addresses associated with the above BTC account (i.e., Dove's BTC account) engaged in multiple transactions with a BTC address within The Website cluster between on or about November 16, 2016, and on or about August 23, 2017. *Id.* at ¶ 29.

- Dove purchased the Subject Premises (which, again, was tied to Dove's BTC account) in 2011, had a Florida's driver's license registered to that address at the time of the warrant (as did another adult), and listed the Subject Premises as the registered address for both his former and current businesses. *Id.* at ¶¶ 31, 32, 34 n.10. Furthermore, vehicles associated with Dove and the Subject Premises (including one for which he was the primary driver) were observed at the Subject Premises in the weeks leading up to the submission of the affidavit. *Id.* at ¶¶ 34-39.

- Individuals who have a sexual interest in children or images of children and who utilize the web to access with the intent to view, possess, receive, or distribute images of child pornography almost always possess and maintain their child pornographic materials "for many years" in the privacy and security of their homes or some other secure locations. *Id.* at ¶¶ 41(c), (d), 42.

As these averments demonstrate, even without paragraph 30, there was probable cause to believe that Dove took numerous steps to access and use The Website and its content, most of which consisted of child pornography. These steps

included downloading Tor software, accessing the darknet, locating The Website's web address, creating an account with The Website by providing a username and password, and—in order to acquire “points” for downloading videos—authorizing (through the use of his private key) the transmittal of BTC from BTC addresses within his BTC account to a BTC address that The Website specifically assigned to him. Furthermore, as averred by Special Agent Garcia, Dove engaged in not just one but multiple such BTC transactions with The Website over a roughly nine-month period between November 2016 and August 2017.

In light of these averments, there was a “fair probability” that evidence, contraband, and/or property relating to the distribution, receipt, and/or possession of child pornography would be found at Dove's residence (i.e., the Subject Premises) at the time the issuing magistrate judge signed the warrant. The fact that these averments (in the absence of paragraph 30) do not include a direct allegation that Dove actually downloaded child pornography does not lead to a different conclusion. *United States v. Orr*, \_\_\_ F. App'x \_\_\_, 2020 WL 3564626, at \*6 (11th Cir. July 1, 2020) (per curiam) (“Probable cause for child pornography offenses does not depend on law enforcement having proof that child pornography is in the defendant's possession.”) (citing *United States v. Williams*, 444 F.3d 1286, 1304 n.87 (11th Cir. 2006) (explaining that several courts have held that affidavits indicating a defendant has joined internet groups where members exchange child pornography provide probable cause to search his home, although there was no evidence of any downloads of illegal child pornography), *overturned on other grounds by* 553 U.S. 285



(2008)); *United States v. Schwinn*, 376 F. App'x 974, 978-79 (11th Cir. 2010) (per curiam) (“Evidence that a person paid for access to multiple websites determined to contain child pornography—at least one of which had conspicuous descriptions identifying the website’s content as, at least in part, containing child pornography—supports the inference that the person used the websites and therefore possessed some of the contents of those websites.”) (citations omitted); *United States v. Taylor*, 250 F. Supp. 3d 1215, 1230-31 (N.D. Ala. 2017) (noting “several circuit courts have held that membership in a child pornography website alone sufficiently establishes probable cause, reasoning that an individual who took the affirmative steps necessary to become a member probably accessed or contributed to the site’s illegal content” and citing *United States v. Shields*, 458 F.3d 269, 278 (3d Cir. 2006); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004)), *aff’d*, 935 F.3d 1279 (11th Cir. 2019), *as corrected*, (Sept. 4, 2019).

In an effort to convince the Court otherwise, Dove asserted at the most recent hearing that, without paragraph 30, probable cause is lacking because The Website contained adult pornography in addition to child pornography. This argument is unavailing. As noted above, the probable cause inquiry deals with probabilities, not certainties. *Brinegar*, 338 U.S. at 175; *United States v. Arguelles*, 2018 WL 2123557, at \*4 (N.D. Fla. May 8, 2018) (“The probable cause standard does not require certainty, a preponderance of the evidence, or even a prima facie showing of criminal activity. [Instead, o]nly a ‘fair probability’ of criminality is required. . . .”) (citing *Gates*, 462 U.S. at 235). It is clear from Special Agent Garcia’s affidavit that The

Website principally peddled child pornography and actively discouraged the uploading of adult pornography. As such, the allegation that the BTC addresses affiliated with Dove's BTC account engaged in multiple BTC transactions with a BTC address within The Website cluster over an extended time period, when read in conjunction with the remainder of the affidavit other than paragraph 30, is sufficient to uphold the warrant on review.

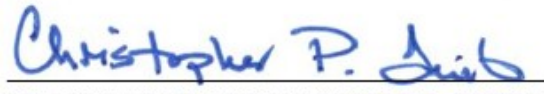
V.

The law instructs that courts should look at search warrant affidavits as a whole and in a realistic, commonsense, and non-technical manner, giving faith to the words and phrases in the affidavits in the context in which they were written. *Gates*, 462 U.S. at 236; *Joyce*, 2012 WL 7148366, at \*2. Dove's examination of Special Agent Garcia's affidavit, pursued with the benefit of hindsight and sometimes seizing on the agent's minor semantic choices, exceeds the review the Court must conduct in this case. While I recognize that Special Agent Garcia's affidavit is not perfect, "perfection is neither the standard nor the question; the court is [instead] bound by the standards set forth in *Franks*." *United States v. Moreland*, 2010 WL 4269145, at \*6 (M.D. Ala. June 25, 2010), *report and recommendation adopted*, 2010 WL 4269144 (M.D. Ala. Oct. 27, 2010).

Here, Dove has failed to make the requisite showing under *Franks* that Special Agent Garcia made an intentional or reckless false statement or omission. And, even if he had made such a showing, I find that the probable cause analysis would not change if the search warrant affidavit were modified as Dove suggests.

Accordingly, I recommend that Dove's *Motion for a Hearing Pursuant to Franks v. Delaware* (Doc. 83) be denied.

Respectfully submitted this 4th day of September 2020.

  
HONORABLE CHRISTOPHER P. TUIITE  
United States Magistrate Judge

**NOTICE TO PARTIES**

A party has fourteen (14) days from this date to file written objections to the Report and Recommendation's factual findings and legal conclusions. A party's failure to file written objections, or to move for an extension of time to do so, waives that party's right to challenge on appeal any unobjected-to factual finding(s) or legal conclusion(s) the District Judge adopts from the Report and Recommendation. *See* 11th Cir. R. 3-1; 28 U.S.C. § 636(b)(1).

Copies to:  
Honorable Charlene E. Honeywell, United States District Judge  
Counsel of record